

(corresponding to
US 2003/0126457 A1)

⑨

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-198527

(43)Date of publication of application : 11.07.2003

(51)Int.Cl.

H04L 9/08

G06F 12/14

G06K 19/00

H04L 9/32

(21)Application number : 2001-397629

(71)Applicant : FUJITSU LTD

(22)Date of filing : 27.12.2001

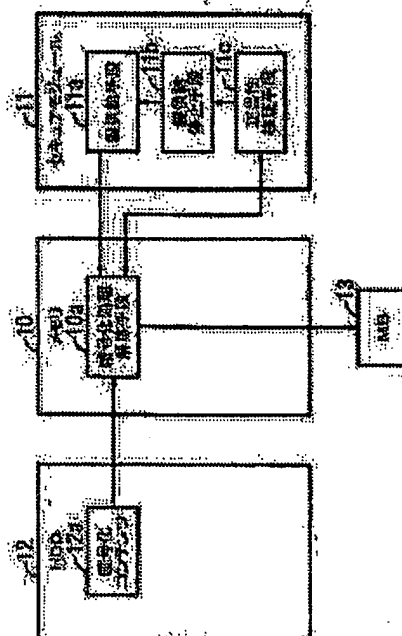
(72)Inventor : KOBAYAMA KIYOYUKI
HASEBE TAKAYUKI

(54) INFORMATION REPRODUCING DEVICE AND SECURE MODULE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve safety in an information reproducing device having an open architecture.

SOLUTION: A secure module 11 has a structure in which it is impossible to refer to internally stored information from the outside. a memory 10 has a structure in which reference from the outside is enabled. An enciphering processing cancel means 10a is packaged on the memory 10 and cancels enciphering processing applied to information by using a prescribed key. A key supply means 11a is packaged on the secure module 11 and supplies the key to the enciphering processing cancel means 10a. A correctness verifying means 11c is packaged on the secure module 11, supplies prescribed information to the enciphering processing cancel means 10a and verifies correctness of the enciphering processing cancel means 10a by referring to information answered as a result. A key supply stop means 11b is packaged on the secure module 11 and when correctness is not verified by the correctness verifying means 11c, key supply means 11a is stopped.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2003-198527

(P2003-198527A)

(43)公開日 平成15年7月11日(2003.7.11)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	H 0 4 L 9/00	6 0 1 B 5 B 0 3 5
G 0 6 K 19/00		G 0 6 K 19/00	Q 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 E
			6 0 1 A

審査請求 未請求 請求項の数10 O L (全 18 頁)

(21)出願番号 特願2001-397629(P2001-397629)

(22)出願日 平成13年12月27日(2001.12.27)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 小桧山 清之

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72)発明者 長谷部 高行

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74)代理人 100092152

弁理士 服部 毅巖

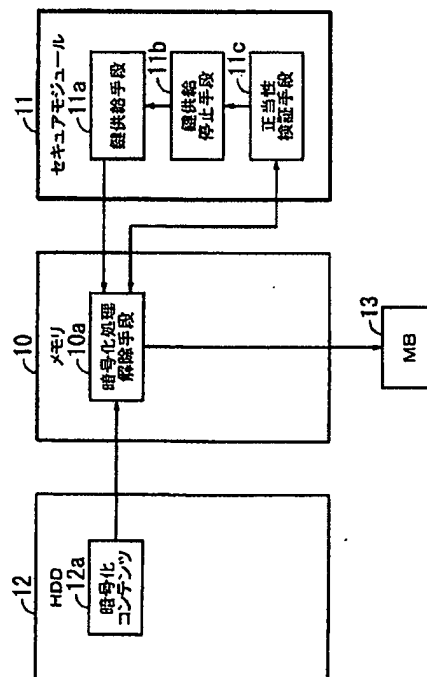
最終頁に続く

(54)【発明の名称】 情報再生装置およびセキュアモジュール

(57)【要約】

【課題】 オープンアーキテクチャーを有する情報再生装置の安全性を高める。

【解決手段】 セキュアモジュール11は、内部に格納されている情報を外部から参照することができない構造を有する。メモリ10は、外部から参照することが可能な構造を有する。暗号化処理解除手段10aは、メモリ10上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。鍵供給手段11aは、セキュアモジュール11上に実装され、暗号化処理解除手段10aに対して鍵を供給する。正当性検証手段11cは、セキュアモジュール11上に実装され、暗号化処理解除手段10aに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段10aの正当性を検証する。鍵供給停止手段11bは、セキュアモジュール11上に実装され、正当性検証手段11cによって正当性が認められない場合には、鍵供給手段11aによる鍵の供給を停止する。



【特許請求の範囲】

【請求項1】 伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、

内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、
外部から参照することが可能なメモリと、
前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、

前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、
前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、
前記セキュアモジュール上に実装され、前記正当性検証手段によって正当性が認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、
を有することを特徴とする情報再生装置。

【請求項2】 前記正当性検証手段は、前記暗号化処理解除手段に対して供給する前記所定の情報の初期値を、装置が起動されるたびに変更することを特徴とする請求項1記載の情報再生装置。

【請求項3】 前記正当性検証手段は、前記暗号化処理解除手段の正当性を検証するためのプロトコルを複数有しており、所定の周期で前記プロトコルを変更することを特徴とする請求項1記載の情報再生装置。

【請求項4】 前記鍵供給手段は、前記暗号化処理解除手段からの返答が所定の時間以上無い場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする請求項1記載の情報再生装置。

【請求項5】 前記メモリまたはセキュアモジュール上に実装されている複数の手段は、暗号化された状態で記録媒体に予め記録されており、必要に応じて暗号化が解除され、前記メモリまたはセキュアモジュール上に実装されることを特徴とする請求項1記載の情報再生装置。

【請求項6】 前記メモリ上に実装されている前記暗号化処理解除手段は、メモリ上に実装される度に、実現形態が異なることを特徴とする請求項1記載の情報再生装置。

【請求項7】 前記暗号化処理解除手段によって暗号化が解除された情報を外部に出力するための出力手段と、
前記暗号化処理解除手段によって暗号化が解除された情報を、前記出力手段に供給する際に、再度暗号化する暗号化手段と、

を更に有することを特徴とする請求項1記載の情報再生装置。

【請求項8】 前記暗号化手段は、複数の暗号化プロトコルから所定のプロトコルを選択して暗号化を行うこと

を特徴とする請求項7記載の情報再生装置。

【請求項9】 前記セキュアモジュールは着脱可能なデバイスによって構成されていることを特徴とする請求項1記載の情報再生装置。

【請求項10】 伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、

10 前記情報再生装置は、

外部から参照することが可能なメモリと、
前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、

前記セキュアモジュールは、
前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、
前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、

20 前記セキュアモジュール上に実装され、前記正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、

を有することを特徴とするセキュアモジュール。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は情報再生装置およびセキュアモジュールに関し、特に、伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置および伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールに関する。

【0002】

【従来の技術】近年、ブロードバンドインターネットやデジタル放送が普及しつつあり、配信されたコンテンツ（主にデジタルAVコンテンツ）の安全性を保障する権利保護技術がクローズアップされている。この中でも特にパーソナルコンピュータ（PC：Personal Computer）はオープンアーキテクチャーであり、基本的に誰でも覗き見ができるため、安全性の実現は困難とされている。

【0003】しかし、一方でパーソナルコンピュータは、ブロードバンドインターネットの主要な出入り口であり、そこで安全性を保証できれば、インターネット全体でのデジタルAVコンテンツの配信が可能になり意義は大きい。

【0004】従来は、パーソナルコンピュータのソフト上での権利保護は、安全性を保障するアルゴリズムの秘匿化、さらにアルゴリズムの解析を困難にする難読化が主流であった。しかしパーソナルコンピュータ上のソフトは、一旦、メインメモリ上に実装してしまえば、コピーすることは容易であり、コピーした結果を時間かけて解析することで、権利保護アルゴリズムを解析できる。非常に安全性に不安のある権利保護システムと考えられ、放送等公共性の高いシステムで一度解析されたことによる被害を考えると採用は困難である。

【0005】図10は、パーソナルコンピュータを用いた従来のシステムの構成例を示す図である。この図に示すように、従来のシステムは、パーソナルコンピュータ50、ネットワーク51、スピーカ52、表示装置53、および、入力装置54によって構成されている。

【0006】パーソナルコンピュータ50は、CPU (Central Processing Unit) 50a、ROM (Read Only Memory) 50b、RAM (Random Access Memory) 50c、HDD (Hard Disk Drive) 50d、MB (Multimedia Board) 50f、I/F (Interface) 50g、50h、および、バス50iによって構成され、ネットワーク51を介してダウンロードした情報を復号化してスピーカ52および表示装置53に出力する。

【0007】ここで、CPU50aは、HDD50dに格納されているプログラムに従って各種演算処理を実行するとともに、装置の各部を制御する。ROM50bは、CPU50aが実行する基本的なプログラムやデータを格納している。

【0008】RAM50cは、CPU50aが各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。HDD50dは、CPU50aが実行するプログラムやデータ等を格納している。

【0009】MB50fは、CPU50aから供給された符号化された音声データや画像データを復号し、もとの音声信号や画像信号を生成して、スピーカ52および表示装置53に出力する。

【0010】I/F50gは、ネットワーク51を介して情報を送受信する際のインターフェースであり、プロトコル変換やデータのフォーマット変換を実行する。I/F50hは、入力装置54から供給されたデータを、パーソナルコンピュータ50の内部形式のデータに変換する。

【0011】バス50iは、CPU50a、ROM50b、RAM50c、HDD50d、MB50f、および、I/F50g、50hを相互に接続し、これらの間で情報の授受を可能にする。

【0012】ネットワーク51は、例えば、インターネットによって構成されており、ネットワーク上に接続されているサーバ等との間で情報を送受信する。スピーカ52は、MB50fから供給された音声信号に対応する

音声に変換して出力する。

【0013】表示装置53は、例えば、CRT (Cathode Ray Tube) モニターや液晶モニターによって構成されており、MB50fから供給された画像信号を画像として表示する。

【0014】入力装置54は、例えば、マウスやキーボードによって構成されており、ユーザの操作に応じた情報を発生して出力する。図11は、図10に示すパーソナルコンピュータ50における情報の流れを示す図である。

【0015】この図に示すように、HDD50dには、基本ソフト、暗号解読鍵群、および、暗号化コンテンツが格納されている。ここで、基本ソフトは、暗号化コンテンツの暗号を解除するための処理等を行うためのソフトウェアであり、悪意あるユーザに解読されるのを防止するために、難読化されている。ここで、難読化とは、以下のような処理が施されていることをいう。

【0016】難読化前 $X = X + Y$

難読化後 $X = X * 2 + 1 + Y * 2 - 1$

$X = X \div 2$

即ち、難読化前と後で演算結果は同じであるが、難読化後はアルゴリズムを解析するのが困難になっている。

【0017】暗号解読鍵群は、暗号化コンテンツに施されている暗号を解読するための複数の鍵であり、悪意あるユーザに容易に取得されないようにするために、秘密のスクランブルが施され、また、秘密の場所に格納されている。

【0018】暗号化コンテンツは、暗号化処理が施されたコンテンツであり、例えば、画像、音声、コンピュータデータ等から構成されている。暗号化コンテンツの再生が開始されると、以下の処理が実行される。

【0019】(1) HDD50dから難読化されている基本ソフトが読み出され、RAM50c上に実装される。

(2) その後、読み出された基本ソフトは、必要に応じて秘密の場所に格納され、秘密のスクランブルがかかった暗号解読鍵がHDD50dから読み出される。暗号解読鍵は例えば、3~5箇所に分けて秘密の格納場所に格納され、更に、秘密の演算等を施さないと目的の鍵が得られないように処理されている。

【0020】(3) 暗号化コンテンツが読み出され、暗号解読鍵で暗号が解読される。

(4) 続いて、暗号解読されたコンテンツが圧縮されている場合には、伸張処理(ビデオコンテンツの場合はMPEG伸張処理、オーディオコンテンツの場合はMPEGオーディオ伸張処理など)が実行され、得られたデータがRAM50c上の画像バッファおよび音声バッファに格納された後、MB50fに出力される。

【0021】(5) MB50fは、供給された音声データをD/A変換処理するとともに、画像データに従って

描画処理を実行し、得られた音声信号をスピーカ52へ出力し、一方、画像信号を表示装置53に出力する。

【0022】

【発明が解決しようとする課題】しかし、このような処理において、基本ソフトはパーソナルコンピュータ50のRAM50cに実装されるので、悪意のあるユーザによって解読されたり、コピーされたりする危険性を伴う。仮に、HDD50dに格納されている基本ソフトその他を全て暗号化したとしても、その暗号を解くためのソフトがパーソナルコンピュータ50のどこかに存在すれば、そのソフトを解析して鍵の保存場所が特定されると、やはり基本ソフトは解析され権利保護アルゴリズムが判明してしまう。

【0023】放送等、公共性の高い網では、アルゴリズムが判明しても容易にコンテンツの解読ができない処理法が望まれる。現行のハードウェア主体のデジタルテレビ受信機では、MULTI2、DES(Data Encryption Standard)などの暗号化が行われている。これらは、アルゴリズムは公知であるが、「暗号解読鍵」が判明しない限り、コンテンツの暗号を解読することは不可能である。

【0024】しかし「暗号解読鍵」は、ハードウェアに内蔵され、ソフトウェア上には読み出すことはできないような構造となっている。更に、暗号解読回路やコンテンツ処理回路(MPEGビデオ伸張やMPEGオーディオ伸張)もハードウェアで構成されているため、処理の内容を覗き見るのは極めて困難である。このため、ハードウェア主体のデジタル放送受信機は安全とされ、このようなシステムは実際に商用化が進んでいる。日本のパーフェクトTV(商標)や米国のDirectTV(商標)などはこのような受信機の好例である。

【0025】これに対しソフトウェア処理では、「暗号解読鍵」、「暗号解読回路」、「コンテンツ処理回路(MPEGビデオ伸張やMPEGオーディオ伸張)」がソフトであり、こうした基本ソフト自体、さらには途中の演算結果も容易に読み取り可能なパーソナルコンピュータ50上のRAM50cに実装されるため、解析、覗き見が容易に行われてしまうという問題点があった。

【0026】本発明はこのような状況に鑑みてなされたものであり、パーソナルコンピュータ等のオープンアーキテクチャを有する装置に対して最低限のハードウェアを付加することで安全なソフトウェア処理を可能とする情報再生装置およびそのようなセキュアモジュールを提供することを目的とする。

【0027】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示す、伝送媒体によって伝送されてきた情報または記録媒体(HDD12)に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造

を有するセキュアモジュール11と、外部から参照することが可能なメモリ10と、前記メモリ10上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段10aと、前記セキュアモジュール11上に実装され、前記暗号化処理解除手段10aに対して前記鍵を供給する鍵供給手段11aと、前記セキュアモジュール11上に実装され、前記暗号化処理解除手段10aに対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段10aの正当性を検証する正当性検証手段11cと、前記セキュアモジュール11上に実装され、前記正当性検証手段11cによって正当性が認められない場合には、前記鍵供給手段11aによる鍵の供給を停止する鍵供給停止手段11bと、を有する情報再生装置が提供される。

【0028】ここで、セキュアモジュール11は、内部に格納されている情報を外部から参照することができない構造を有する。メモリ10は、外部から参照することが可能な構造を有する。暗号化処理解除手段10aは、メモリ10上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。鍵供給手段11aは、セキュアモジュール11上に実装され、暗号化処理解除手段10aに対して鍵を供給する。正当性検証手段11cは、セキュアモジュール11上に実装され、暗号化処理解除手段10aに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段10aの正当性を検証する。鍵供給停止手段11bは、セキュアモジュール11上に実装され、正当性検証手段11cによって正当性が認められない場合には、鍵供給手段11aによる鍵の供給を停止する。

【0029】また、本発明では上記課題を解決するために、伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、前記情報再生装置は、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、前記セキュアモジュールは、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とするセキュアモジュールが提供される。

【0030】ここで、情報再生装置において、メモリ

は、外部から参照することが可能な構成を有する。暗号化処理解除手段は、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する。一方、セキュアモジュールにおいて、鍵供給手段は、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する。正当性検証手段は、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する。鍵供給停止手段は、セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、鍵供給手段による鍵の供給を停止する。

【0031】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は、本発明の動作原理を説明する原理図である。この図に示すように、本発明の情報再生装置は、メモリ10、セキュアモジュール11、HDD12、および、MB13によって構成されている。

【0032】ここで、メモリ10は、例えば、RAMによって構成されており、ソフトウェアによって実現される暗号化処理解除手段10aが実装されている。セキュアモジュール11は、例えば、PCカードによって構成されている。このセキュアモジュール11は、TRM (Tamper Resistant Module) 構造を有しているため、外部から覗き見を防止するとともに、内部のデータが改竄されることを防止することができる。

【0033】なお、セキュアモジュール11には、鍵供給手段11a、鍵供給停止手段11b、正当性検証手段11cが実装されている。ここで、鍵供給手段11aは、暗号化処理解除手段10aに対して暗号化を解除するための鍵を供給する。

【0034】正当性検証手段11cは、暗号化処理解除手段10aに対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段10aの正当性を検証する。

【0035】正当性検証手段11cによって暗号化処理解除手段10aが正当であると認められない場合には、鍵供給手段11aによる鍵の供給を停止する。MB13は、メモリ10上に実装されている暗号化処理解除手段10aによって暗号化が解除されたコンテンツを取得し、音声信号および画像信号に変換してスピーカおよび表示装置に供給する。

【0036】次に、以上の原理図の動作について説明する。セキュアモジュール11は、着脱可能なモジュールであり、例えば、鍵供給手段11a、鍵供給停止手段11b、正当性検証手段11cが実装された状態で、情報再生装置本体に装着することができる。

【0037】メモリ10に実装されている暗号化処理解除手段10aは、セキュアモジュール11に予め格納しておき、これを起動時にメモリ10に転写するか、ある

いは、HDD12に暗号化した状態で格納しておき、起動時にメモリ10に転写し、そこでセキュアモジュール11に格納されている鍵を用いて暗号化処理を解除する。

【0038】このような状態において、再生が開始されると、まず、正当性検証手段11cは、暗号化処理解除手段10aに対して秘密の情報を供給する。暗号化処理解除手段10aは、秘密の情報を取得し、これに所定の処理を施すことにより、所定の情報を得る。そして、得られた情報を正当性検証手段11cに供給する。

【0039】正当性検証手段11cは、暗号化処理解除手段10aから返答された情報を参照し、暗号化処理解除手段10aの正当性を検証する。その結果、暗号化処理解除手段10aが正当であると認められる場合は、鍵供給手段11aから暗号化処理解除手段10aに対して暗号化を解除するための鍵が供給される。

【0040】一方、暗号化処理解除手段10aが正当であると認められない場合は、鍵供給停止手段11bは、鍵供給手段11aから暗号化処理解除手段10aへの鍵の供給を停止させる。

【0041】暗号化処理解除手段10aの正当性が確認された場合には、暗号化処理解除手段10aは、鍵供給手段11aから供給された鍵を用いて、HDD12から読み出した暗号化コンテンツ12aの暗号化を解除し、MB13に供給する。

【0042】MB13は、暗号化処理解除手段10aから供給された、暗号化が解除されたコンテンツに含まれている音声データおよび画像データをそれぞれ音声信号および画像信号に変換し、図示せぬスピーカと、表示装置に供給する。

【0043】再生処理が開始された後も、セキュアモジュール11の正当性検証手段11cは、暗号化処理解除手段10aに対して所定の周期で秘密の情報を供給し、その返答としての情報を検証することにより、暗号化処理解除手段10aが不正にコピーされたり改竄されたりすることを防止する。

【0044】以上に示したように、本発明の情報再生装置では、外部から覗き見することができないセキュアモジュール11を設け、ここを起点としてメモリ10に実装されている暗号化処理解除手段10aの正当性を検証し、正当性が確認できた場合には、鍵を供給するようにしたので、オープンアーキテクチャを採用するパーソナルコンピュータ等においても、最小限のハードウェアを追加することにより、セキュリティを向上させることが可能になる。

【0045】また、正当性検証手段11cにより、暗号化処理解除手段10aの正当性を定期的に検証するようにしたので、メモリ10に実装されている暗号化処理解除手段10aが不正に解析され、成りすまし等の改竄行為の発生を防止することが可能になる。

【0046】次に、本発明の実施の形態について説明する。図2は、本発明の実施の形態の構成例を示す図である。この図に示すように、本発明の情報再生装置を含むシステムは、パーソナルコンピュータ（情報再生装置）50、ネットワーク51、スピーカ52、表示装置53、および、入力装置54によって構成されている。

【0047】パーソナルコンピュータ50は、CPU50a、ROM50b、RAM50c、HDD50d、セキュアモジュール50e、MB50f、I/F（Interface）50g、50h、および、バス50iによって構成され、ネットワーク51を介してダウンロードした情報を復号化してスピーカ52および表示装置53に出力する。

【0048】ここで、CPU50aは、HDD50dに格納されているプログラムに従って各種演算処理を実行するとともに、装置の各部を制御する。ROM50bは、CPU50aが実行する基本的なプログラムやデータを格納している。

【0049】RAM50cは、CPU50aが各種演算処理を実行する際に、実行対象となるプログラムやデータを一時的に格納する。HDD50dは、CPU50aが実行するプログラムやデータ等を格納している。

【0050】セキュアモジュール50eは、例えば、PC-CARD等によって構成されており、ユーザの正当性を確認するための情報が格納されている。なお、セキュアモジュール50eは、TRM構造を有しているもので、外部から覗き見を防止するとともに、内部のデータが改竄されることを防止することができる。

【0051】MB50fは、CPU50aから供給された符号化された音声データや画像データを復号し、もとの音声信号や画像信号を生成して、スピーカ52および表示装置53に出力する。

【0052】I/F50gは、ネットワーク51を介して情報を送受信する際のインターフェースであり、プロトコル変換やデータのフォーマット変換を実行する。I/F50hは、入力装置54から供給されたデータを、パーソナルコンピュータ50の内部形式のデータに変換する。

【0053】バス50iは、CPU50a、ROM50b、RAM50c、HDD50d、セキュアモジュール50e、MB50f、および、I/F50g、50hを相互に接続し、これらの間でデータの授受を可能にする。

【0054】ネットワーク51は、例えば、インターネットによって構成されており、ネットワーク上に接続されているコンテンツサーバ等との間で情報を送受信する。スピーカ52は、MB50fから供給された音声信号を対応する音声に変換して出力する。

【0055】表示装置53は、例えば、CRTモニターや液晶モニターによって構成されており、MB50fか

ら供給された画像信号を画像として表示する。入力装置54は、例えば、マウスやキーボードによって構成されており、ユーザの操作に応じた情報を発生して出力する。

【0056】図3は、図2に示す実施の形態における情報の流れを示す図である。この図に示すように、HDD50dには、暗号化暗号解読鍵群、暗号化ソフト群、暗号化プロトコル群、および、暗号化コンテンツが格納されている。

【0057】ここで、暗号化暗号解読鍵群は、暗号化コンテンツの暗号化を解除するための鍵の集合である。暗号化ソフト群は、暗号化を解除するための基本ソフトの集合である。

【0058】暗号化プロトコル群は、暗号を解読する基本ソフトに対して挿入され、基本ソフトの正当性を検証するためのプロトコルの集合である。暗号化コンテンツは、暗号化されたコンテンツであり、例えば、暗号化された音声データや画像データによって構成されている。

【0059】一方、セキュアモジュール50eには、マスター鍵群、送信/返信受信ソフト、および、その他のソフトが存在する。ここで、マスター鍵群は、暗号化コンテンツを解読するための暗号化された鍵の集合である。

【0060】送信/返信受信ソフトは、RAM50c上に実装されている送信受信/返信ソフトとの間で情報を授受し、その正当性を検証する。また、その他のソフトは、例えば、プロトコルの初期値を変更するソフト、暗号化暗号の鍵を解読するための暗号化暗号解読ソフト、任意の暗号化ソフト、任意の暗号化プロトコルを解読する任意暗号化プロトコル解読ソフト、任意のプロトコルを組み込むための任意プロトコル組み込みソフト、ソフトウェアをダウンロードするためのソフトウェアダウンロードソフト、暗号化コンテンツを解読するための暗号化コンテンツ解読ソフト、コンテンツを再度暗号化するためのコンテンツ再暗号化ソフト、コンテンツの暗号解読用の鍵を送信するためのコンテンツ暗号解読鍵送信ソフト、および、再暗号化されたコンテンツを送信するための再暗号化コンテンツ送信ソフトによって構成されている。

【0061】RAM50cには、セキュアソフトが格納されており、このセキュアソフトには、基本ソフトが含まれる。基本ソフトには、送信受信/返信ソフト、メモリ領域変更ソフト、コンテンツ暗号解読鍵受信ソフト、再暗号化コンテンツ解読ソフト、コンテンツ処理ソフト、および、デコード画像コンテンツ出力ソフトが含まれている。

【0062】ここで、送信受信/返信ソフトは、セキュアモジュール50eからの送信を受信し、適当な応答を返す。メモリ領域変更ソフトは、セキュアモジュール50eからの送信を受信し秘匿化必要データ（暗号解読

鍵、暗号解読後のMPEGビデオ／オーディオコンテンツ、MPEGビデオ／オーディオ伸張後の情報格納領域など）が使用するメモリ領域を変更する。

【0063】コンテンツ暗号解読鍵受信ソフトは、コンテンツの暗号を解読するための鍵を受信する。再暗号化コンテンツ解読ソフトは、セキュアモジュール50eにおいて再暗号化されたコンテンツを解読するための鍵を受信する。

【0064】コンテンツ処理ソフトは、MPEGビデオ伸張ソフト、MPEGオーディオ伸張ソフト等によって構成されている。デコード画像コンテンツ出力ソフトは、コンテンツ処理ソフトによって得られた画像コンテンツ等をMB50fに対して出力する。

【0065】MB50fでは、音声情報に対しては、D/A変換処理等が施され、また、画像情報に対しては描画処理等が実行される。次に、本発明の実施の形態の動作の概要について以下に説明する。

【0066】本実施の形態において、権利保護を行うための基本的な仕組みは以下の通りである。即ち、セキュアモジュール50eから毎回セキュアソフトをRAM50cにロードする。ロードしたセキュアソフトには、セキュアソフトの安全性を確認するための秘密の番号等を送信／受信するためにプロトコルが存在し、これがリアルタイムに通信することで安全性を確認する。

【0067】その時、セキュアソフトをコピーされ、安全性確認用の秘密の番号などを解析されるのを防ぐため、以下の対策を実行する。

(1) セキュアモジュール50eにタイマーを設け、送信／受信の間隔があまり長い場合はセキュアソフト改竄の可能性があるものとして、セキュアモジュール50eからの暗号解読鍵提供の停止などの処置を講じる。

【0068】(2) また、セキュアソフトをコピーされ、成りすまされるのを防止するため、同じ秘密の番号等が2度返信された場合等は、セキュアモジュール50eからの暗号解読鍵提供の停止などの処置を講じる。

【0069】(3) 更に、毎回、例えば1時間程度の間隔で、セキュアソフト自体を置換する。このためにセキュアモジュール50e内、あるいは、HDD50d内に複数（実際には無数）のセキュアソフトを準備し、その都度、異なるセキュアソフトをロードする。セキュアソフトの機能は同じであるが、安全性を確認するプロトコルや秘密の番号を毎回変更するようにする。このような構成により、例えば、一度はセキュアソフトを解析されても、セキュアソフトの内容は毎回異なるので実質的に解析は不可能になる。基本的に1時間でセキュアソフトを解析し、演算結果等をファイル出力するように改竄するのは不可能と考えられるので、安全性は十分確保できる。

【0070】なお、セキュアソフトの内容変更は、例えば送信、受信プロトコルのみを変更することで比較的簡

単に行える。また、プロトコルの中の初期変数などを変えるだけでも変更を容易に実現することができる。

【0071】例えば、以下のような秘密の番号を生成するプログラムを用いることにより、安全性確認用の送信、受信機能を実現できる。

$$X = X + Y * Z * X$$

ここで、Xは秘密の番号とし、YとZは秘密の番号を生成するための初期変数である。X、Y、Zの値を任意に変更するだけで無数の安全性確認プロトコルが生成できる。X=1、Y=3、Z=5とすると、Xは、以下のように変化する。

【0072】X=1、16、16+16×15、・・・もちろん、以上はほんの一例であり、このように簡単な方法では、初期値を変更してもRAM50cが接続されているPCIバスを介して内容を解析される可能性があるもので、これ以外にも別の式を上の式に重畳させるのも良い。また、特別な一覧表によりXがある値になったら強制的に他の値に変換する等の処理を行えば、基本式が漏洩した場合でも安全性は保てる。

【0073】更に、ソフトを解析してこの式が判明しても、例えば、1時間毎にセキュアソフト自体を変更するようにすれば、解析が非常に困難になる。次に、以上の実施の形態の具体的な動作について説明する。このシステムの動作は以下の通りである。

【0074】(1) 所定のコンテンツを視聴しようとする場合には、ユーザは、電源を投入し、入力装置54を操作して、表示装置53に表示されている所定のアイコンをクリックする。

【0075】(2) すると、セキュアモジュール50eが起動し、HDD50d内の複数の暗号化基本ソフトからランダムに一つを読み出す。

(3) 次に、暗号化基本ソフトをセキュアモジュール50e内の暗号解読鍵と暗号解読ソフトで解読する。

【0076】(4) 次に、複数の暗号化プロトコルの中からランダムに適当なものを1つあるいは複数読み出し、セキュアモジュール50e内の暗号解読鍵と暗号解読ソフトで解読する。

【0077】(5) 暗号解読後の基本ソフトに暗号解読後の1つあるいは複数のプロトコルを挿入し、セキュアソフトを作成する。

(6) 1つあるいは複数のプロトコルのそれぞれの初期値を初期化する。

【0078】(7) 初期化されたセキュアソフトをRAM50cにロード（ダウンロード）し、セキュアソフトを起動する。セキュアモジュール50eは、セキュアソフトがロードされ、起動されるとセキュアモジュール50e内のタイマーを参照して、あまり期間をおかずに（セキュアソフトの成りすましを防ぐため、時間をおかない）秘密の番号がセキュアソフトから、通信プロトコルに従って送信されるのを確認する。

【0079】(8)セキュアモジュール50eは、返しの秘密の番号を送信する。

(9)セキュアモジュール50eは、更にまた秘密の番号が返信されるのを待つ。

【0080】(10)セキュアモジュール50eは、内蔵されているタイマーを参照し、秘密の番号の返信に一定以上の時間がかかった場合は、セキュアソフトが改竄されたと見なし、セキュアソフトにエラー信号を渡して動作を停止させる。また、同一の秘密の番号が連続して返信された場合にも、セキュアソフトが改竄されたと見なし、セキュアソフトにエラー信号を渡して動作を停止させるようにしてもよい。

【0081】(11)一方、一定時間内に正常な返信があった場合には、セキュアモジュール50eは、セキュアソフトの動作が正常とみなす。

(12)セキュアモジュール50eは、HDD50dから暗号化コンテンツを読み出し、暗号解読鍵を使って解読する。

【0082】(13)セキュアモジュール50eは、暗号解読コンテンツを再暗号化する。

(14)セキュアモジュール50eは、再暗号化コンテンツをセキュアソフトに送信する。

【0083】(15)セキュアモジュール50eは、更に、別のプロトコルでセキュアソフトの安全性をさらに確認後、再暗号化コンテンツ解読鍵をセキュアソフトに送信する。

【0084】(16)セキュアモジュール50eは、コンテンツの再生が終了するか、または、終了の指示がユーザからなされるまで、上記(8)～(16)の処理を繰り返す。

【0085】一方、セキュアソフトは、以下の処理を実行する。

(1)セキュアソフトは、秘密の番号の送信受信を通してセキュアモジュール50eから再暗号化コンテンツと再暗号化コンテンツ解読用の鍵を受信する。

【0086】(2)セキュアソフトは、受信した再暗号化コンテンツ解読用の鍵を用いてコンテンツの解読を行う。

(3)セキュアソフトは、暗号解読の結果を、秘密の番号等の送信受信で決定された秘密のメモリ領域に対して、排他的論理和演算等の簡単なスクランブルを施した後に格納する。なお、格納先のメモリ領域は常時変更することにより、情報の漏洩を防止する。また、セキュアソフトが使用するレジスタについては、その都度変更するようにすれば、レジスタを媒介として内部の動作を解析されることを防止することができる。更に、秘密の番号を送受信する際には、割り込み禁止フラグをセットすることにより、他のソフトの割り込みを禁止し、割り込みによって内部の動作を解析されることを防止できる。なお、「秘密の番号の送受信」以外でも、解析を困難に

する必要があるあらゆる箇所でこのように割り込み禁止フラグを活用することができる。

【0087】(4)セキュアソフトは、格納された暗号解読されたコンテンツがMPEG圧縮された画像データであるなら以下のようにMPEGビデオ伸張処理を施す。また、MPEG圧縮音声データであるならMPEGオーディオ伸張処理を施す。また、データ放送、字幕情報等のコンテンツであるなら、それに応じた別の処理ルーチンに転送する。

10 【0088】(5)セキュアソフトは、処理済みのコンテンツが、例えば、MPEG画像データである場合は、処理結果をRAM50c上のバッファ領域に格納する。なお、RAM50c上の固定された領域に格納するようにすると、覗き見される可能性があるので、格納番地は、セキュアモジュール50eとの交信によって設定される常時変化する番地に格納する。なお、格納番地を変更する以外にも、例えば、格納時にセキュアモジュール50eとの交信によって設定される常時変化するスクランブル方法を採用することも可能である。

20 【0089】(6)格納されたMPEGビデオデコード結果は、DMA (Dynamic Memory Access) 転送等でMB50fにAGPバス等を介し転送され、MB50fにおいてA/D変換処理を行い、モニター等で再生できる形式に変換されて表示される。なお、音声データの場合も基本的に同じような処理を経てスピーカに転送されて再生される。

30 【0090】以上の実施の形態によれば、TRM構成を有するセキュアモジュール50eにより、RAM50c上に実装されている基本ソフトの正当性を検証するようにしたので、オープンアーキテクチャーを有するシステムの安全性を高めることが可能になる。

【0091】また、正当性を検証するためのプロトコルを所定の周期で変更するようにしたので、基本ソフトが覗き見された場合においても、安全性を確保することが可能になる。

【0092】次に、本発明の第2の実施の形態について説明する。図4は、本発明の第2の実施の形態の構成例について説明する図である。この図に示すように、本発明の第2の実施の形態は、HDD50dに格納される情報を減少させ、その代わりにセキュアモジュール50eのメモリ領域に権利保護情報を格納したことを特徴としている。

40 【0093】この例では、HDD50dに格納されているのは、暗号化されたデジタルAVコンテンツ等のみである。一方、セキュアモジュール50eには、(1)暗号化コンテンツを解読するための暗号化された鍵の集合であるマスター鍵群、(2)各プロトコル内秘密番号の計算式の初期値変更ソフト、(3)ソフト群、(4)プロトコル群、(5)任意プロトコルをセキュアソフト
50 に組込むソフト、(6)RAM50cへ任意プロトコル

組込回路セキュアソフトをダウンロードするソフト、

(7) セキュアソフトに送信／返信受信し、セキュアソフトの安全性を確認するためのソフト、(8) コンテンツ暗号解読鍵を送信するソフトが存在する。また、この他にも図示せぬタイマーを具備し、送信後の受信期間を測定し一定以上の期間が過ぎた場合はセキュアソフトへのコンテンツ暗号解読鍵の送信を停止する。

【0094】RAM50cには、セキュアソフトが格納されており、このセキュアソフトには、基本ソフトが含まれる。基本ソフトには、以下のソフトが含まれている。即ち、基本ソフトには、(1) 基本ソフトを受信するためのソフト、(2) 送信受信／返信ソフト、(3) メモリ領域を変更するためのメモリ領域変更ソフト、

(4) コンテンツ暗号解読鍵を受信するためのコンテンツ暗号解読鍵受信ソフト、(5) 暗号化コンテンツを解読するための暗号化コンテンツ解読ソフト、(6) コンテンツ処理ソフト、(7) デコード画像コンテンツ出力ソフトが格納されている。

【0095】また、セキュアモジュール50e、HDD50d、RAM50cは、汎用のPCIバスで相互に接続されて情報を交換し、RAM50cとMB50fはAGPバス等のローカルバス（汎用バスと違い、傍受不可能）で接続される。

【0096】次に、以上の実施の形態の動作について説明する。このシステムの動作は以下の通りである。

(1) デジタル放送をPC画面上で視聴したい場合、ユーザは、電源を投入した後、表示装置53に表示されているデジタル放送受信用のアイコンをクリックする。

【0097】(2) セキュアモジュール50eが起動し、モジュール内の複数の基本ソフトからランダムに1つを読み出す。

(3) セキュアモジュール50eは、次に、複数のプロトコルの中からランダムに適当なものを1つまたは複数読み出し、基本ソフトに1つまたは複数のプロトコルを挿入し、セキュアソフトを作成する。

【0098】(4) セキュアモジュール50eは、1つまたは複数のプロトコル上の初期値などを初期化する。

(5) セキュアモジュール50eは、初期化されたセキュアソフトをRAM50cにロード（ダウンロード）し、セキュアソフトを起動する。

【0099】(6) セキュアモジュール50eは、セキュアソフトがロードされ、起動されるとセキュアモジュール内のタイマーを参照し、所定の時間（セキュアソフトの成りすましを防ぐため短時間とする）が経過すると秘密の番号がセキュアソフトから、通信プロトコルに従って送信されるのを確認する。

【0100】(7) セキュアモジュール50eは、返しの秘密の番号を生成して送信する。

(8) セキュアモジュール50eは、秘密の番号が返信

されるのを待つ。

(9) セキュアモジュール50eは、タイマーを参照し、秘密の番号の返信に一定以上の時間がかかる場合には、セキュアソフトが改竄された可能性があるとし、セキュアソフトにエラー信号を渡して動作を停止させる。

【0101】(11) 一方、一定時間内に正常な返信が返った場合は、セキュアモジュール50eは、セキュアソフトの動作が正常とみなし、更に、別のプロトコルでセキュアソフトの安全性を確認した後、暗号化コンテンツ解読鍵をセキュアソフトに送信する。

【0102】(12) セキュアモジュール50eは、この後は、上記(8)～(12)の処理を繰り返す。一方、RAM50c上のセキュアソフトは、以下の処理を実行する。

【0103】(1) セキュアモジュールとの秘密の番号の送信受信を通してHDD50dから暗号化コンテンツを受信する。

(2) セキュアソフトは、セキュアモジュール50eから暗号化コンテンツ解読用の鍵を受信する。

【0104】(3) セキュアソフトは、受信した鍵を用いて受信したコンテンツの暗号解読を行う。

(4) セキュアソフトは、暗号を解読した結果に対して、例えば、排他的論理和によるスクランブルを施した後、秘密の番号等の送受信によって決定された秘密のメモリ番地に格納する。なお、格納先のメモリ番地は、固定するのではなく、格納の度に変更するようにすることが望ましい。

【0105】(5) セキュアソフトは、暗号解読されたコンテンツは、もしそれがMPEG圧縮された画像データなら以下のようにMPEG画像伸張処理が施される。MPEG圧縮音声データならMPEG音声伸張処理が施される。また、データ放送、字幕情報等のコンテンツなら、それに応じた別の処理ルーチンに転送される。

【0106】(6) セキュアソフトは、処理されたコンテンツを、例えば、MPEG画像データの場合には、RAM50cのパッファー領域に転送する。なお、RAM50cの固定された番地に格納すると、覗き見される可能性があるので、格納番地は、セキュアモジュール50eとの送受信の際に設定される番地（常に変化する番地）に格納される。なお、格納時にセキュアモジュールとの交信の中で設定される方法に基づいて、コンテンツをスクランブル処理するようにしてもよい。

【0107】(7) セキュアソフトは、格納されたMPEG画像データを、DMA転送等でMB50fにAGPバス等を介し転送し、MB50fによりA/D変換して、表示装置53で再生可能な形式に変換する。

【0108】(9) セキュアソフトは、音声データについても、前述の画像データの場合と同様の処理により復号し、スピーカ52に転送して再生する。以上に説明し

たように、本発明の第2の実施の形態では、マスター鍵等の情報についても、セキュアモジュール50eに格納するようにしたので、HDD50dに格納する第1の実施の形態と比較して、セキュリティを更に向上させることが可能になる。

【0109】次に、本発明の第3の実施の形態について説明する。図5は、本発明の第3の実施の形態の構成例を示す図である。この図に示すように、本発明の第3の実施の形態では、図3に示す実施の形態と比較すると、RAM50cにスクランブル処理ソフトが追加されており、また、MB50fにデスクランブル処理ソフトが追加されている。その他の構成は、図3の場合と同様であるので、その説明は省略する。

【0110】ここで、スクランブル処理ソフトは、MP E Gデコード処理等が施されたコンテンツに対して、所定のスクランブル処理を施す。一方、デスクランブル処理ソフトは、RAM50cにおいてスクランブル処理が施されたコンテンツに対してデスクランブル処理を施し、もとの情報を再生する。

【0111】次に、以上の実施の形態の動作について簡単に説明する。HDD50dおよびセキュアモジュール50eでは、前述の場合と同様の処理により、鍵の送受信が行われた後、基本ソフトをRAM50c上にダウンロードしてそこに実装する。

【0112】RAM50cは、ダウンロードされた基本ソフトにより、セキュアモジュール50eを介して暗号化コンテンツを受信し、暗号を解除する。そして、スクランブル処理ソフトは、暗号が解除されたコンテンツに対して所定のスクランブル処理を施し、MB50fに対して送信する。

【0113】MB50fは、RAM50cから送信されてきたスクランブルが施されたコンテンツを受信し、対応するデスクランブルソフトがデスクランブル処理を施し、もとのコンテンツデータを再生する。

【0114】そして、得られたコンテンツデータが音声信号である場合には、D/A変換処理によりアナログ信号に変換してスピーカ52に出力する。また、得られたコンテンツデータが画像データである場合には、描画処理により画像を描画した後、映像信号に変換し、表示装置53に出力する。

【0115】以上のような実施の形態によれば、RAM50cからMB50fに供給されるコンテンツデータを不正に取り出すといった行為を防止することができる。次に、本発明の第4の実施の形態について説明する。

【0116】図6は、本発明の第4の実施の形態の構成例を示す図である。この図に示す実施の形態では、図5に示す場合と比較して、セキュアモジュール50eに通信プロトコル送信ソフトが追加され、また、MB50fに通信プロトコル受信ソフトが追加されている。それ以外は、図5の場合と同様である。

【0117】RAM50cに格納されている通信プロトコル送信ソフトは、コンテンツデータに対するスクランブル方法や、コンテンツデータの出力順序を示す情報（通信プロトコル情報）をMB50fに対して送信する。

【0118】MB50fに格納されている通信プロトコル受信ソフトは、通信プロトコル送信ソフトから送られてきた通信プロトコル情報を受信し、装置内部の該当する部分に供給する。

【0119】次に、以上の実施の形態の動作について簡単に説明する。コンテンツデータの再生が開始されると、セキュアモジュール50eの通信プロトコル送信ソフトは、MB50fに対して通信プロトコル情報を送信する。

【0120】通信プロトコル情報を受信したMB50fは、この情報に含まれているデスクランブル処理ソフトと、コンテンツの出力順序を示す情報とを抽出する。そして、抽出した情報に従ってコンテンツデータの順序を並べ替えするとともに、デスクランブル処理を施す。

【0121】ところで、通信プロトコル情報は、例えば、所定の時間間隔で送信され、送信の度にデスクランブル方法や出力順序が変更される。従って、悪意あるユーザによってRAM50c上に存在するスクランブル処理ソフトが解析された場合であっても、次のタイミングでは異なるスクランブル処理がなされていることから、不正使用を防止することが可能になる。

【0122】次に、本発明の第5の実施の形態の構成例について説明する。図7は、本発明の第5の実施の形態の構成例を示す図である。この図に示すように、本発明の第5の実施の形態は、ディジタル放送受信機の構成例である。

【0123】ここで、図7に示すディジタル放送受信機70は、ディジタルチューナ70a、MULTI2暗号解読部70b、B-CAS（BS Conditional Access Systems）カード70c、ライセンス生成部70d、再暗号化処理部70e、HDD70f、MPEGデコーダ70g、暗号復号部70h、グラフィック処理部70i、再生ライセンス部70j、アナログ著作権保護部70k、および、ディジタル著作権保護部70lによって構成されている。また、その外部には、パラボラアンテナ71が接続されている。

【0124】ここで、ディジタルチューナ70aは、パラボラアンテナ71によって捕捉された衛星からの電波を電気信号（ディジタル信号）に変換して出力する。MULTI2暗号解読部70bは、ディジタルチューナ70aから出力されたディジタル信号に施されているMULTI2暗号を解読し、もとのデータに復号して出力する。

【0125】B-CASカード70cは、ICチップが内蔵されたプラスチック製のカードであり、ユーザの

正当性を保証するための情報が格納されている。ライセンス生成部70dは、再暗号化に必要なライセンス情報を生成し、再暗号化処理部70eに供給する。

【0126】再暗号化処理部70eは、MULTI2暗号解読部70bから供給されたデジタル信号を再度暗号化し、HDD70fに供給する。HDD70fは、再暗号化処理部70eから供給されたデータを所定の領域に格納する。

【0127】暗号復号部70hは、HDD70fから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。MPEGデコーダ70gは、暗号復号部70hから供給されたデータに対してMPEGデコード処理を施し、画像データおよび音声データを生成する。

【0128】グラフィック処理部70iは、MPEGデコーダ70gから出力された画像データ等に基づいて描画処理を行い、もとの画像信号に変換して出力する。再生ライセンス部70jは、暗号復号部70hにおいて暗号を復号する際のライセンス情報を供給する。

【0129】アナログ著作権保護部70kは、アナログ信号としての画像信号に対してコピー防止用の信号を重畳して出力する。デジタル著作権保護部70lは、デジタル信号としての画像信号暗号化して出力する。

【0130】なお、この実施の形態においては、太線で示されている機能ブロック（ライセンス生成部70d、再暗号化処理部70e、および、再生ライセンス部70j）は、TRMによって構成され、内部の情報を参照することができない構造となっている。

【0131】また、機能ブロック間の結線であって、破線で示されている結線は、権利保護のために外部接続が禁止されている結線である。次に、以上の実施の形態の動作について説明する。

【0132】パラボラアンテナ71によって捕捉された衛星からの電波は、デジタルチューナ70aに供給され、そこで、MPEG-TSデジタルストリームに変換されて出力される。

【0133】MPEG-TSストリームには、複数の情報がMULTI2暗号化された上で時分割多重化されており、MULTI2暗号解読部70bは、B-CASカード70cから供給された暗号鍵等のライセンス情報を参照し、MPEG-TSデジタルストリーム中の視聴者が選択した番組（特定デジタルAVコンテンツ）を復号する。

【0134】再暗号化処理部70eは、ライセンス生成部70dから供給されるライセンス情報を参照し、AVコンテンツを再暗号化し、HDD70fの所定の領域に格納する。

【0135】暗号復号部70hは、HDD70fに格納された暗号化デジタルAVコンテンツを再生する場合、再生ライセンス部70jから暗号を復号するための

ライセンス情報を取得し、暗号の復号処理を実行し、もとのAVコンテンツを生成する。

【0136】MPEGデコーダ70gは、暗号復号部70hによって復号されたAVコンテンツに対してMPEGデコード処理を施しもとの画像データを再生し、グラフィック処理部70iに供給する。

【0137】グラフィック処理部70iは、MPEGデコーダ70gから供給された画像データに基づいて描画処理等のグラフィック処理を実行し、画像信号を生成する。そして、得られた画像信号をアナログ著作権保護部70kとデジタル著作権保護部70lに供給する。

【0138】アナログ著作権保護部70kは、グラフィック処理部70iから供給された画像信号の所定の部分に不正コピーを防止するための信号を重畳し、モニターに対して出力する。

【0139】デジタル著作権保護部70lは、グラフィック処理部70iから供給された画像信号に対して暗号化処理を施し、モニターに対して出力する。ところで、以上の実施の形態においては、前述したように、太線で示す機能ブロック（ライセンス生成部70d、再暗号化処理部70e、および、再生ライセンス部70j）はTRM構造を有している。従って、図1に示すように、これらの機能ブロックに対して、鍵供給手段11a、鍵供給停止手段11b、および、正当性検証手段11cに該当する機能を設け、正当性を所定の時間間隔で検証するとともに、正当性が確認できない場合には、鍵の供給を停止するようにすれば、悪意のユーザによって受信したコンテンツが不正に使用されることを防止することができる。

【0140】次に、本発明の第6の実施の形態について説明する。図8は、本発明の第6の実施の形態の構成例を示す図である。この図に示すように、本発明の第6の実施の形態は、デジタルチューナ80a、MULTI2暗号解読部80b、B-CASカード80c、再暗号化ライセンス生成部80d、HDD80e、ソフト暗号復号再生ライセンス部80f、ソフトMPEGデコーダ80g、ソフトAAC (Advanced Audio Coding) デコーダ80h、グラフィック処理部80i、音声処理部80j、HDCP (High-bandwidth Digital Content Protection) LSI80kによって構成されている。また、その外部には、パラボラアンテナ81が接続されている。

【0141】ここで、デジタルチューナ80aは、パラボラアンテナ81によって捕捉された衛星からの電波を電気信号（デジタル信号）に変換して出力する。MULTI2暗号解読部80bは、デジタルチューナ80aから出力されたデジタル信号に施されているMULTI2暗号を解読し、もとのデータに復号して出力する。

【0142】B-CASカード80cは、ICチップが

内蔵されたプラスチック製のカードであり、ユーザの正当性を保証するための情報が格納されている。再暗号化ライセンス生成部80dは、再暗号化に必要なライセンス情報を生成し、再暗号化処理を実行する。

【0143】HDD80eは、再暗号化ライセンス生成部80dから供給されたデータを所定の領域に格納する。ソフト暗号復号再生ライセンス部80fは、再生ライセンスを生成し、この再生ライセンスに従って、HDD80eから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。

【0144】ソフトMPEGデコーダ80gは、ソフト暗号復号再生ライセンス部80fから供給されたAVコンテンツに対してMPEGデコード処理を施し、画像データを生成する。

【0145】ソフトAACデコーダ80hは、音声信号を復号し、もとの音声データを生成して出力する。グラフィック処理部80iは、ソフトMPEGデコーダ80gから供給された画像データに対してグラフィック処理を施し、得られた画像信号をHDCP LSI80kに出力する。

【0146】HDCP LSI80kは、グラフィック処理部80iから供給された画像信号に対してHDCP処理を施し、出力する。音声処理部80jは、ソフトAACデコーダ80hから出力される音声データをD/A変換して出力する。

【0147】なお、以上の実施の形態において、太線で示されている機能ブロック（B-CASカード80c、再暗号化ライセンス生成部80d、ソフト暗号復号再生ライセンス部80f）は、TRMによって構成され、内部の情報を参照することができない構造となっている。

【0148】また、ソフト暗号復号再生ライセンス部80f、ソフトMPEGデコーダ80g、および、ソフトAACデコーダ80hは、ソフトウエアによって構成されている。

【0149】従って、TRMによって構成された部分を、図1に示すセキュアモジュール11とし、ソフトウエアによって構成された部分を、図1に示すメモリ10に対応付け、必要な機能を具備することにより、前述の場合と同様に悪意のユーザによって受信したコンテンツが不正に使用されることを防止することができる。

【0150】次に、本発明の第7の実施の形態について説明する。図9は、本発明の第7の実施の形態の構成例を示す図である。この図に示すように、本発明の第7の実施の形態は、デジタルチューナ90a、MULTI2暗号解読部90b、B-CASカード90c、再暗号化ライセンス生成部90d、HDD90e、ソフト暗号復号再生ライセンス部90f、ソフトMPEGデコーダ90g、ソフトAACデコーダ90h、グラフィック処理部90i、音声処理部90j、HDCP LSI90kによって構成されている。また、その外部には、パラ

ボラアンテナ91が接続されている。なお、この実施の形態では、MULTI2暗号解読部90b、再暗号化ライセンス生成部90d、ソフト暗号復号再生ライセンス部90f、ソフトMPEGデコーダ90g、ソフトAACデコーダ90h、グラフィック処理部90i、および、音声処理部90jは、LSIの内部に封入されている。

【0151】ここで、デジタルチューナ90aは、パラボラアンテナ91によって捕捉された衛星からの電波を対応する電気信号（デジタル信号）に変換して出力する。

【0152】MULTI2暗号解読部90bは、デジタルチューナ90aから出力されたデジタル信号に施されているMULTI2暗号を解読し、もとのデータに復号して出力する。

【0153】B-CASカード90cは、ICチップが内蔵されたプラスチック製のカードであり、ユーザの正当性を保証するための情報が格納されている。再暗号化ライセンス生成部90dは、再暗号化に必要なライセンス情報を生成し、再暗号化処理部を実行する。

【0154】HDD90eは、再暗号化ライセンス生成部90dから供給されたデータを所定の領域に格納する。ソフト暗号復号再生ライセンス部90fは、再生ライセンスを生成し、この再生ライセンスに従って、HDD90eから読み出されたデータに施されている暗号を復号し、もとのデータを生成する。

【0155】ソフトMPEGデコーダ90gは、ソフト暗号復号再生ライセンス部90fから供給されたAVコンテンツに対してMPEGデコード処理を施し、画像データを生成する。

【0156】ソフトAACデコーダ90hは、音声信号を復号し、もとの音声データを生成して出力する。グラフィック処理部90iは、ソフトMPEGデコーダ90gから供給された画像データに対してグラフィック処理を施し、得られた画像信号をHDCP LSI90kに出力する。

【0157】HDCP LSI90kは、グラフィック処理部90iから供給された画像信号に対してHDCP処理を施し、出力する。音声処理部90jは、ソフトAACデコーダ90hから出力される音声データをD/A変換して出力する。

【0158】なお、以上の実施の形態において、ソフト暗号復号再生ライセンス部90f、ソフトMPEGデコーダ90g、および、ソフトAACデコーダ90hは、ソフトウエアによって構成されている。

【0159】従って、LSIによって構成された部分を、図1に示すセキュアモジュール11とし、ソフトウエアによって構成された部分を、図1に示すメモリ10に対応付け、必要な機能を具備することにより、前述の場合と同様に悪意のユーザによって受信したコンテンツ

が不正に使用されることを防止することができる。

【0160】更に、本実施の形態では、ソフトウェアによって構成された部分もLSIの内部に封入するようにしたので、更にセキュリティを向上させることが可能になる。

【0161】なお、以上の実施の形態に示すブロック図は、ほんの一例であり、本発明がこのような場合のみに限定されるものではないことはいうまでもない。また、以上の実施の形態において、ソフトウェアによって構成される部分は、適宜ハードウェアによって置換することが可能であることはいうまでもない。

【0162】(付記1) 伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、前記正当性検証手段によって正当性が認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とする情報再生装置。

【0163】(付記2) 前記正当性検証手段は、前記暗号化処理解除手段に対して供給する前記所定の情報の初期値を、装置が起動されるたびに変更することを特徴とする付記1記載の情報再生装置。

【0164】(付記3) 前記正当性検証手段は、前記暗号化処理解除手段の正当性を検証するためのプロトコルを複数有しており、所定の周期で前記プロトコルを変更することを特徴とする付記1記載の情報再生装置。

【0165】(付記4) 前記鍵供給手段は、前記暗号化処理解除手段からの返答が所定の時間以上無い場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする付記1記載の情報再生装置。

【0166】(付記5) 前記鍵供給手段は、前記暗号化処理解除手段から同一の返答が連続してなされた場合には、正当性が確認できないとして、前記鍵の供給を停止することを特徴とする付記1記載の情報再生装置。

【0167】(付記6) 前記メモリまたはセキュアモジュール上に実装されている複数の手段は、暗号化された状態で記録媒体に予め記録されており、必要に応じて暗号化が解除され、前記メモリまたはセキュアモジュール上に実装されることを特徴とする付記1記載の情報再生装置。

【0168】(付記7) 前記メモリ上に実装されている前記暗号化処理解除手段は、メモリ上に実装される度に、実現形態が異なることを特徴とする付記1記載の情報再生装置。

【0169】(付記8) 前記実現形態は、実装されるメモリ上の領域であることを特徴とする付記7記載の情報再生装置。

(付記9) 前記実現形態は、使用するメモリの領域であることを特徴とする付記7記載の情報再生装置。

10 【0170】(付記10) 前記実現形態は、使用するレジスタの種類であることを特徴とする付記7記載の情報再生装置。

(付記11) 前記暗号化処理解除手段によって暗号化が解除された情報を外部に出力するための出力手段と、前記暗号化処理解除手段によって暗号化が解除された情報を、前記出力手段に供給する際に、再度暗号化する暗号化手段と、を更に有することを特徴とする付記1記載の情報再生装置。

20 【0171】(付記12) 前記暗号化手段は、複数の暗号化プロトコルから所定のプロトコルを選択して暗号化を行うことを特徴とする付記11記載の情報再生装置。

(付記13) 前記暗号化手段は、前記セキュアモジュールに格納されているプログラムを前記メモリ上に実装することにより実現されることを特徴とする付記12記載の情報再生装置。

30 【0172】(付記14) 前記メモリ上に実装される複数の手段は、その実行時に割り込み禁止フラグを立て、他のプログラムの割り込みが発生することを禁止することを特徴とする付記1記載の情報再生装置。

【0173】(付記15) 前記セキュアモジュールに格納されているプログラムを、前記メモリ上に実装する際には、毎回異なる暗号化を施してメモリに供給することを特徴とする付記1記載の情報再生装置。

【0174】(付記16) 前記セキュアモジュールは着脱可能なデバイスによって構成されていることを特徴とする付記1記載の情報再生装置。

40 (付記17) 伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、前記情報再生装置は、外部から参照することが可能なメモリと、前記メモリ上に実装され、前記情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、前記セキュアモジュールは、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して前記鍵を供給する鍵供給手段と、前記セキュアモジュール上に実装され、前記暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、前記暗号化処理解除手段の正

当性を検証する正当性検証手段と、前記セキュアモジュール上に実装され、前記正当性検証手段によって正当であると認められない場合には、前記鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を有することを特徴とするセキュアモジュール。

【0175】

【発明の効果】以上説明したように本発明では、伝送媒体によって伝送されてきた情報または記録媒体に格納されている情報を再生する情報再生装置において、内部に格納されている情報を外部から参照することができない構造を有するセキュアモジュールと、外部から参照することが可能なメモリと、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する鍵供給手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する正当性検証手段と、セキュアモジュール上に実装され、正当性検証手段によって正当性が認められない場合には、鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を設けるようにしたので、オープンアーキテクチャー構成を有する、例えば、パーソナルコンピュータにより情報を再生する場合においても、最小限のハードウェアを追加することにより、安全なシステムを構築することができる。

【0176】また、本発明では、伝送媒体によって伝送されてきた情報または記録媒体に蓄積されている情報を再生する情報再生装置に着脱可能に実装され、情報を再生する際のセキュリティに関する処理を実行するセキュアモジュールにおいて、情報再生装置は、外部から参照することが可能なメモリと、メモリ上に実装され、情報に施されている暗号化処理を所定の鍵を用いて解除する暗号化処理解除手段と、を有し、セキュアモジュールは、セキュアモジュール上に実装され、暗号化処理解除手段に対して鍵を供給する鍵供給手段と、セキュアモジュール上に実装され、暗号化処理解除手段に対して所定の情報を供給し、その結果として返答される情報を参照し、暗号化処理解除手段の正当性を検証する正当性検証手段と、セキュアモジュール上に実装され、正当性検証手段によって正当であると認められない場合には、鍵供給手段による鍵の供給を停止する鍵供給停止手段と、を設けるようにしたので、情報再生装置に装着した場合に、最小限の構成でありながら、システムの安全性を高めることができるセキュリティモジュールを提供することが可能になる。

【図面の簡単な説明】

【図1】本発明の動作原理を説明する原理図である。

【図2】本発明の実施の形態の構成例を示す図である。

【図3】図2に示す実施の形態における情報の流れを示

す図である。

【図4】本発明の第2の実施の形態における情報の流れを示す図である。

【図5】本発明の第3の実施の形態における情報の流れを示す図である。

【図6】本発明の第4の実施の形態における情報の流れを示す図である。

【図7】本発明の第5の実施の形態の構成例を示す図である。

【図8】本発明の第6の実施の形態の構成例を示す図である。

【図9】本発明の第7の実施の形態の構成例を示す図である。

【図10】パーソナルコンピュータを用いた従来のシステムの構成例を示す図である。

【図11】図10に示すパーソナルコンピュータにおける情報の流れを示す図である。

【符号の説明】

- 10 メモリ
- 10a 暗号化処理解除手段
- 11 セキュアモジュール
- 11a 鍵供給手段
- 11b 鍵供給停止手段
- 11c 正当性検証手段
- 12 HDD
- 12a 暗号化コンテンツ
- 50 パーソナルコンピュータ
- 50a CPU
- 50b ROM
- 50c RAM
- 50d HDD
- 50e セキュアモジュール
- 50f MB
- 50g, 50h I/F
- 50i バス
- 51 ネットワーク
- 52 スピーカ
- 53 表示装置
- 54 入力装置
- 70 デジタル放送受信機
- 70a デジタルチューナ
- 70b MULTI2暗号解読部
- 70c B-CASカード
- 70d ライセンス生成部
- 70e 再暗号化処理部
- 70f HDD
- 70g MPEGデコーダ
- 70h 暗号復号部
- 70i グラフィック処理部
- 70j 再生ライセンス部

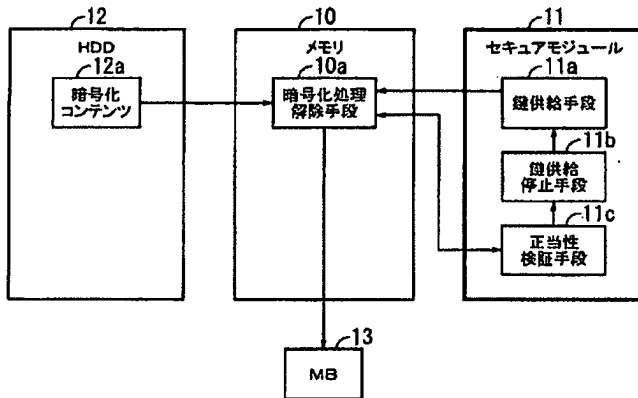
27

70k アナログ著作権保護部
 70l デジタル著作権保護部
 71 パラボラアンテナ
 80 デジタル放送受信機
 80a デジタルチューナ
 80b MULTI2暗号解読部
 80c B-CASカード
 80d 再暗号化ライセンス生成部
 80e HDD
 80f ソフト暗号復号再生ライセンス部
 80g ソフトMPEGデコーダ
 80h ソフトAACデコーダ
 80i グラフィック処理部
 80j 音声処理部
 80k HDCP LSI

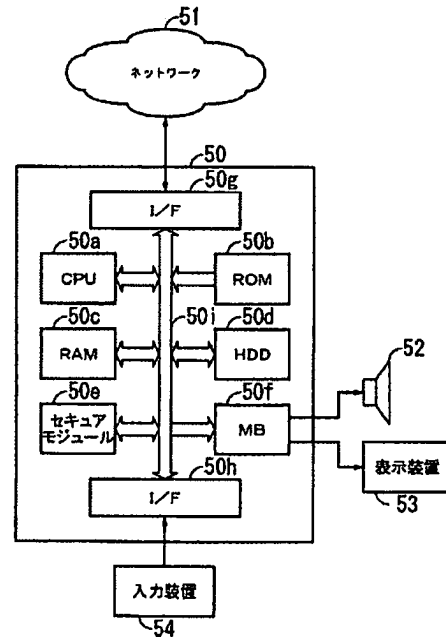
28

81 パラボラアンテナ
 90 デジタル放送受信機
 90a デジタルチューナ
 90b MULTI2暗号解読部
 90c B-CASカード
 90d 再暗号化ライセンス生成部
 90e HDD
 90f ソフト暗号復号再生ライセンス部
 90g ソフトMPEGデコーダ
 90h ソフトAACデコーダ
 90i グラフィック処理部
 90j 音声処理部
 90k HDCP LSI
 91 パラボラアンテナ

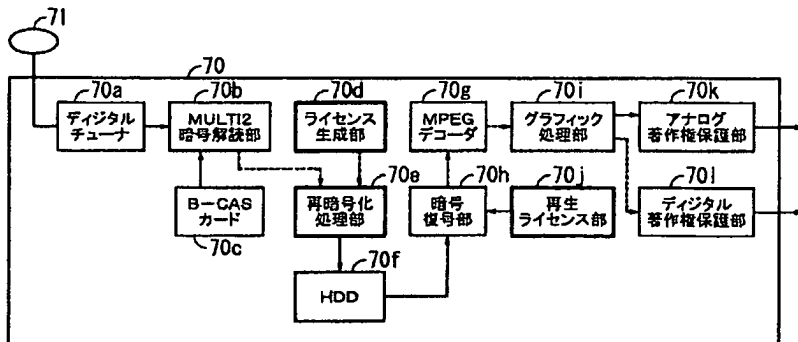
【図1】



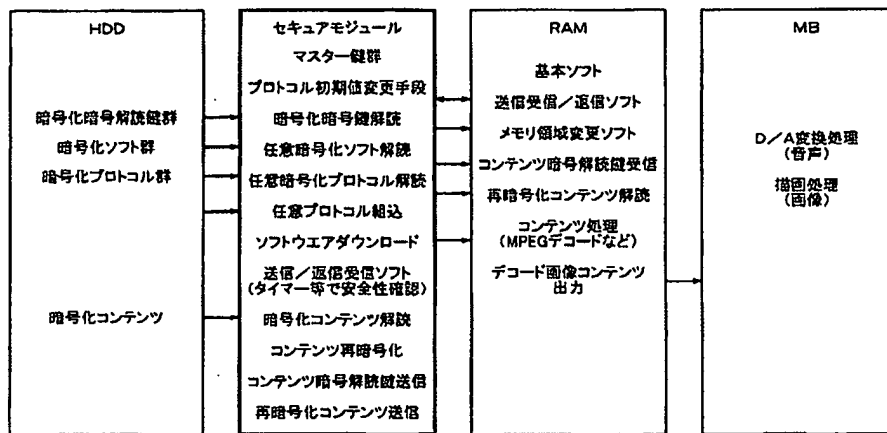
【図2】



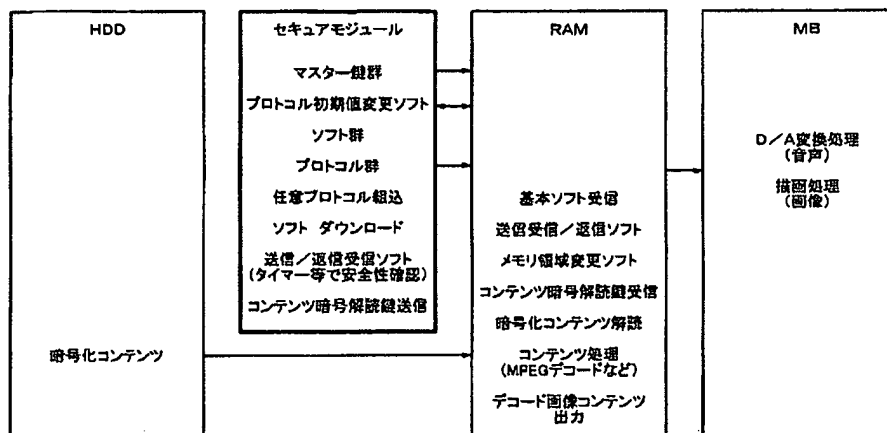
【図7】



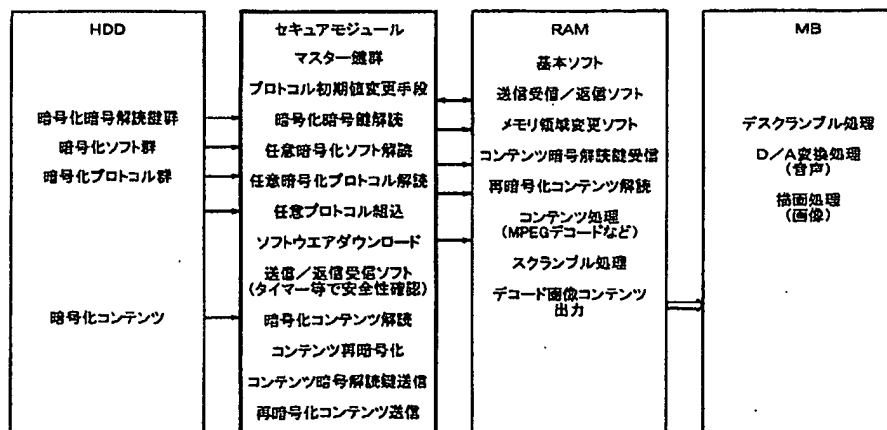
【図3】



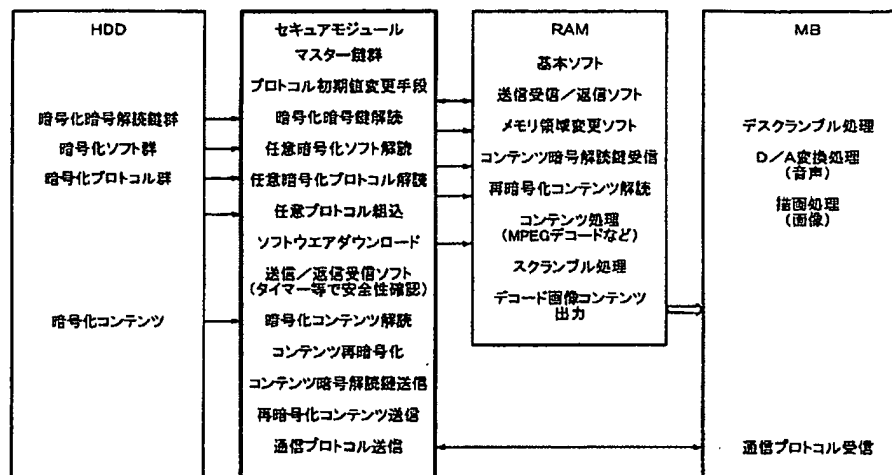
【図4】



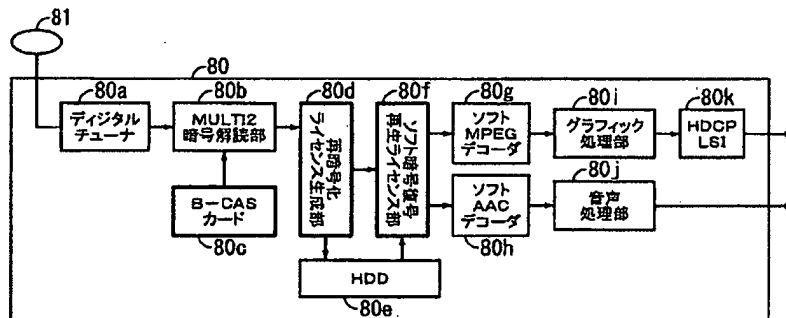
【図5】



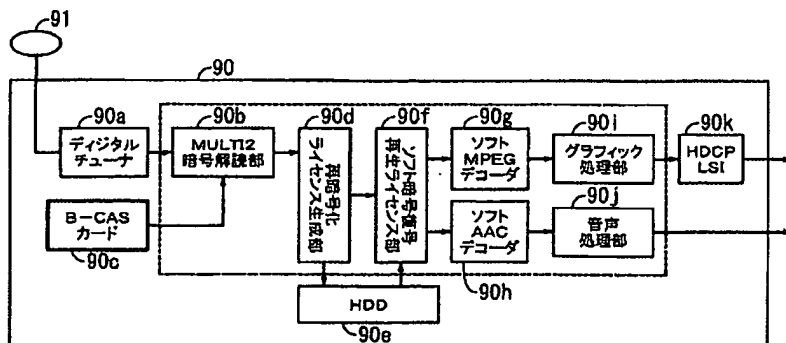
【図6】



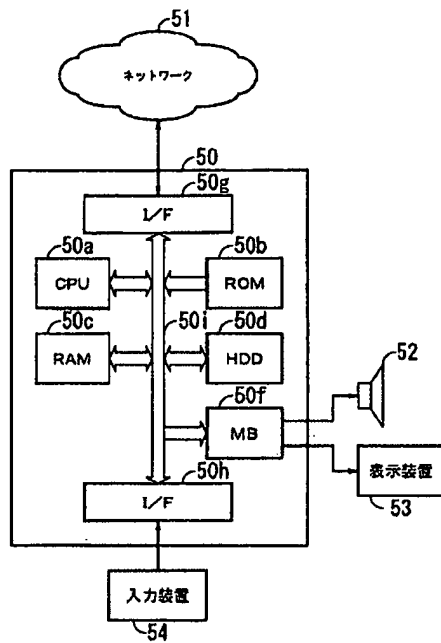
【図8】



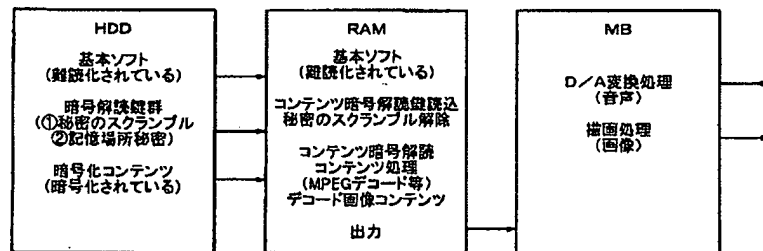
【図9】



【図10】



【図11】



フロントページの続き

Fターム(参考) 5B017 AA03 BA07 BB03 CA07 CA16
 5B035 AA13 BB09 CA11 CA29
 5J104 AA16 AA34